Секція 1

РОЗРОБЛЕННЯ МЕТОДИКИ ТА ЗАСОБІВ ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ ДЛЯ КОМПАНІЙ СЕРЕДНЬОГО ТА МАЛОГО РОЗМІРУ ПРАЦЮЮЧИХ У СФЕРІ ІТ. ЗАБЕЗПЕЧЕННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ТА СЕРЕДОВИЩА

Бутирін Д. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Загрози кібербезпеці швидко зростають, викликаючи серйозні виклики для компаній незалежно від їхнього розміру. Але компанії середнього та малого розміру особливо вразливі через обмежені ресурси та фінансові можливості. Тому виникає необхідність розроблення ефективної методики та засобів, спеціально адаптованих до їхніх потреб і здатних забезпечити надійний рівень захисту інформації та середовища [1].

За даними репорту KHARKIV IT RESEARCH 2021, станом на середину 2021 року тільки в Харкові вели активну діяльність 511 IT-компаній, які співпрацюють з 45 тисячами фахівців різних спеціалізацій. З 2019 року IT-індустрія в Харкові зросла на 29 %, при цьому загалом в Україні працюють 2234 IT-компанії, що зазначено у дашборді технологічної екосистеми України, опублікованому Міністерством цифрової трансформації [2].

З огляду на кількість компаній, які вже працюють та появу нових компаній в сфері IT, та зростаючу кількість загроз, актуальність питання захисту інформації та кібернетичного середовища таких компаній неможливо переоцінити [3,4].

Метою даної роботи є дослідження та визначення основних загроз, ризиків та потреби у засобах захисту інформації та безпеки середовища де ця інформація зберігається, для компаній середнього та малого розміру, які працюють у сфері IT. Також важливим є розроблення комплексного підходу до оцінювання інформаційної та кібербезпеки в таких компаніях, а також створення відповідних засобів захисту.

Основні положення. Під час доповіді зазначається то, що IT компанії отримують від замовників та працюють з великими обсягами інформації. У більшості випадків ця інформація є конфіденційною та дуже вразливою.

Наведені у доповіді результати аналізу потреб компаній, виявлення актуальних загроз і ризиків, дасть змогу ідентифікувати необхідність розроблення інноваційних методик оцінювання, які враховують особливості компаній середнього та малого розміру.

У доповіді визначені критерії оцінювання та наведені розроблені шкали оцінювання, які допоможуть виміряти рівень безпеки та визначити пріоритетні напрямки дій.

У доповіді наведені результати впровадження розробленої методики оцінювання та засобів захисту, яка є ключовим кроком у покращенні безпеки інформації та кібернетичного середовища в компаніях середнього та малого розміру. Її впровадження допоможе зменшити рівень вразливості та ризики, підвищити свідомість та культуру безпеки, а також забезпечити ефективне використання обмежених ресурсів.

Висновки. Беручі до уваги зростання ринку IT в Україні та світі, додавання все більшої кількості IT компаній, які працюють з конфіденційною та вразливою інформацією, можна дійти висновку про абсолютну необхідність розроблення методики та засобів оцінювання інформаційної та кібербезпеки для компаній середнього та малого розміру у сфері IT. Це є дуже важливим завданням та стає дуже актуальним з огляду на стрімке зростання кількості та якості загроз. Такі рішення допоможуть забезпечити надійний рівень захисту інформації та кібернетичного середовища в умовах обмежених ресурсів, а також підвищити відповідність компаній вимогам кібербезпеки.

Список літератури

1. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. *NIST*. URL – https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата звернення 10.09.2023).
2. Kharkiv IT research 2021 — третє масштабне дослідження українського IT-ринку. *IT-Kharkiv*. URL: https://it-kharkiv.com/projects/kharkiv-it-research-2021 (дата звернення 10.09.2023);
3. Cybersecurity Framework - National Institute of Standards and Technology *NIST*. URL – https://www.nist.gov/cyberframework (дата звернення 10.09.2023);
4. CIS Critical Security Controls, Prioritized & simplified best practices, Follow our prioritized set of actions to protect your organization and data from cyber-attack vectors. *Cisecurity*. URL – https://www.cisecurity.org/controls (дата звернення 11.09.2023).

Відомості про авторів

Бутирін Дмитро Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.o.butyrin@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu